

CRS Report for Congress

Received through the CRS Web

Homeland Security: Intelligence Support

Richard A. Best, Jr.
Specialist in National Defense
Foreign Affairs, Defense, and Trade Division

Summary

Legislation establishing a Department of Homeland Security (DHS) (P.L. 107-296) included provisions for an information analysis element within the new department. It did not transfer to DHS existing government intelligence and law enforcement agencies but envisioned an analytical office utilizing the products of other agencies — both unevaluated information and finished reports — to provide warning of terrorist attacks, assessments of vulnerability, and recommendations for remedial actions at federal, state, and local levels, and by the private sector. In January 2003, the Administration announced its intention to establish a new Terrorist Threat Integration Center (TTIC) to undertake many of the tasks envisioned for the DHS informational analysis element, known as Information Analysis and Infrastructure Protection (IAIP), but some Members of Congress argue that TTIC cannot be a substitute for a DHS analytical effort. This report examines different approaches to improving the information analysis function and the sharing of information among federal agencies. It will be updated as circumstances warrant.

Introduction

Better intelligence is held by many observers to be a crucial factor in preventing terrorist attacks. Concerns have been expressed that no single agency or office in the federal government prior to September 11, 2001 was in a position to “connect the dots” between diffuse bits of information that might have provided clues to the planned attacks. Testimony before the two intelligence committees’ Joint Inquiry on the September 11 attacks indicated that significant information in the possession of intelligence and law enforcement agencies was not fully shared with other agencies and that intelligence on potential terrorist threats against the United States was not fully exploited.

For many years, the sharing of intelligence and law enforcement information was circumscribed by administrative policies and statutory prohibitions. Beginning in the

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 23 FEB 2004		2. REPORT TYPE		3. DATES COVERED 00-00-2004 to 00-00-2004	
4. TITLE AND SUBTITLE Homeland Security: Intelligence Support				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Congressional Research Service, The Library of Congress, 101 Independence Ave SE, Washington, DC, 20540-7500				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 6	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

early 1990s, however, much effort has gone into improving interagency coordination.¹ After the September 11 attacks, a number of statutory obstacles were addressed by the USA-Patriot Act of 2001 and other legislation.² Nevertheless, there had been no one place where the analytical effort is centered; the Department of Homeland Security (DHS) was designed to remedy that perceived deficiency as is the Terrorist Threat Integration Center announced by the President in his January 2003 State of the Union address.

Background

The Homeland Security Act (P.L. 107-296), signed on November 25, 2002 established within DHS a Directorate for Information Analysis and Infrastructure Protection (IAIP) headed by an Under Secretary for Information Analysis and Infrastructure Protection (appointed by the President by and with the advice and consent of the Senate) with an Assistant Secretary of Information Analysis (appointed by the President). The legislation, especially the Information Analysis section, seeks to promote close ties between intelligence analysts and those responsible for assessing vulnerabilities of key U.S. infrastructure. The bill envisions an intelligence entity focused on receiving and analyzing information³ from other government agencies and using it to provide warning of terrorist attacks on the homeland to other federal agencies and to state and local officials, and for addressing vulnerabilities that terrorists could exploit.

DHS is not intended to duplicate the collection effort of intelligence agencies; it will not have its own agents, satellites, or signals intercept sites. Major intelligence agencies are not transferred to the DHS, although some DHS elements, including Customs and the Coast Guard, will continue to collect information that is crucial to analyzing terrorist threats.

The legislation establishing DHS envisioned an information analysis element with the responsibility for acquiring and reviewing information from the agencies of the Intelligence Community, from law enforcement agencies, state and local government agencies, and unclassified publicly available information (known as open source information or “osint”) from books, periodicals, pamphlets, the Internet, media, etc. The legislation is explicit that, “Except as otherwise directed by the President, the Secretary [of DHS] shall have such access as the Secretary considers necessary to all information, including reports, assessments, analyses, and unevaluated intelligence relating to threats of terrorism against the United States and to other areas of responsibility assigned by the Secretary, and to all information concerning infrastructures or other vulnerabilities of the

¹ For background on this issue, see CRS Report RL30252, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, by Richard A. Best, Jr.

² See CRS Report RL31377, *The USA Patriot Act: A Legal Analysis*, by Charles Doyle; and CRS Report RL30465, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework*, by Elizabeth Bazan.

³ Some writers distinguish between information and intelligence; the former being unanalyzed information the latter being the result of analysis. In practice, however, the terms are often used interchangeably and the distinction will not be observed in this report.

United States to terrorism, whether or not such information has been analyzed, that may be collected, possessed, or prepared by any agency of the Federal Government.”⁴

DHS analysts are charged with using this information to identify and assess the nature and scope of terrorist threats; producing comprehensive vulnerability assessments of key resources and infrastructure; identifying priorities for protective and support measures by DHS, by other agencies of the federal government, state and local government agencies and authorities, the private sector, and other entities. They are to disseminate information to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the U.S. The intelligence element is also charged with recommending measures necessary for protecting key resources and critical infrastructure in coordination with other federal agencies.

DHS is responsible for ensuring that any material received is protected from unauthorized disclosure and handled and used only for the performance of official duties. (This provision addresses a concern that sensitive personal information made available to DHS analysts could be misused.) As is the case for other federal agencies that handle classified materials, intelligence information is to be transmitted, retained, and disseminated in accordance with policies established under the authority of the Director of Central Intelligence (DCI) to protect intelligence sources and methods and similar authorities of the Attorney General concerning sensitive law enforcement information.⁵

Concerns about DHS Intelligence

Despite enactment of the Homeland Security Act, it is clear that significant concerns persisted within the executive branch about the new department’s ability to analyze intelligence and law enforcement information. Media accounts suggest that these concerns center on DHS’ status as a new and untested agency and the potential risks involved in forwarding “raw” intelligence to the DHS intelligence component.⁶ Another concern is that a new entity, rather than long-established intelligence and law enforcement agencies, would be relied on to produce all-source intelligence relating to the most serious threats facing the country.

⁴ Section 202(a)(1). The language provides for a presidential exception that might arise because of particularly sensitive information; some observers also argue that under any circumstances the President has a constitutional authority to control the dissemination of intelligence information.

⁵ The DCI’s authority for protecting intelligence sources and methods is set forth in 50 USC 403-3(c)(6). The Attorney General’s authorities for safeguarding law enforcement information are diffuse; see, *e.g.*, 18 USC 2511 (interception and disclosure of wire, oral, or electronic communications prohibited, exceptions); 18 USC 2517 (authorization for disclosure and use of intercepted wire, oral, or electronic communications); 21 USC 190(e) (public disclosure of significant foreign narcotics traffickers and required reports, exclusions of certain information).

⁶ See Dan Eggen and John Mintz, “Homeland Security Won’t Have Diet of Raw Intelligence; Rules Being Drafted to Preclude Interagency Conflict,” *Washington Post*, December 6, 2002, p. A43.

DHS Role in the Intelligence Community. The U.S. Intelligence Community consists of the Central Intelligence Agency (CIA) and some 14 other agencies;⁷ it provides information in various forms to the White House and other federal agencies (as well as to Congress). In addition, law enforcement agencies, such as the Federal Bureau of Investigation (FBI), also collect information for use in the federal government.⁸ Within the Intelligence Community, priorities for collection (and to some extent for analysis) are established by the DCI,⁹ based in practice on inter-agency discussions. Being “at the table” when priorities are discussed, it is widely believed, helps ensure equitable allocations of limited collection resources.

The Homeland Security Act makes the DHS information analysis element a member of the Intelligence Community, thus giving DHS a formal role when intelligence collection and analysis priorities are being addressed. DHS officials have indicated that the new Department is actively participating in the process of setting priorities.

The Question of “Raw” Intelligence. There has been discussion in the media whether DHS will have access to “raw” intelligence or only to finished analytical products, but these reports may reflect uncertainty regarding the definition of “raw” intelligence. A satellite photograph standing by itself might be considered “raw” data, but it would be useless unless something were known about where and when it was taken. Thus, satellite imagery supplied to DHS would under almost any circumstances have to include some analysis. The same would apply to signals intercepts. Reports from human agents present special challenges. Some assessment of the reliability of the source would have to be provided, but information that would identify a specific individual is normally retained within a very small circle of intelligence officials so as to reduce the risk of unauthorized disclosure and harm to the source.

The issue of the extent and nature of information forwarded to DHS has proved to be difficult. Reviewing copies of summary reports prepared by existing agencies is seen by some observers as inadequate for the task of putting together a meaningful picture of terrorist capabilities and intentions and providing timely warning. On the other hand, there is a need to ensure that DHS would not be inundated with vast quantities of data and that highly sensitive information is not given wider dissemination than absolutely necessary.

Analytical Quality. The key test for homeland security will of course be the quality of the analytical product — whether terrorist groups can be identified and timely warning given of plans for attacks on the U.S. A critical need exists for trained personnel. The types of information that have to be analyzed come from disparate sources and require a variety of analytical skills that are not in plentiful supply. Academic institutions prepare significant numbers of linguists and area specialists, but training in the inner workings of clandestine terrorist entities is less often undertaken. Analysts with law enforcement backgrounds may not be attuned to the foreign environments from which

⁷ Defined by 50 USC 401a(4).

⁸ 28 USC 533 provides information collecting authority to the Justice Department and the FBI.

⁹ 50 USC 403-3(c)(2).

terrorist groups emerge. In July 2003 DHS had only some 53 analysts and liaison officials with plans to increase this number to about 150.¹⁰

The Terrorist Threat Integration Center

President Bush, in his State of the Union address delivered on January 28, 2003, called for the establishment of a new Terrorist Threat Integration Center (TTIC) that would merge and analyze all threat information in a single location under the direction of the DCI. According to Administration spokesmen, TTIC will eventually encompass CIA's Counterterrorist Center (CTC) and the FBI's Counterterrorism Division, along with elements of other agencies, including DOD and DHS. TTIC's stated responsibilities are to "integrate terrorist-related information collected domestically and abroad" and to provide "terrorist threat assessments for our national leadership."¹¹ On May 1, 2003, TTIC began operations at CIA Headquarters under the leadership of John O. Brennan, who had previously served as the CIA's Deputy Executive Director. By July 2003, it consisted of some 100 analysts and liaison officials with plans to increase to 300 by May 2004.¹²

TTIC appears to be designed to assume at least some of the functions intended for DHS' information analysis division. Representative Cox, chairman of the Select Committee on Homeland Security, has welcomed the establishment of TTIC, while noting that "The establishment of the Center in no way reduces the statutory obligations of the Department [of Homeland Security] to build its own analytic capability."¹³ Making the DCI responsible for TTIC will facilitate its ability to use highly sensitive classified information and TTIC can expand upon the relationships that have evolved in the CTC that was established in CIA's Operations Directorate in the mid-1980s. According to testimony by Administration officials to the Senate Government Affairs Committee on February 26, 2003, TTIC will in effect function as an information analysis center for DHS and DHS will require a smaller number of analysts with less extensive responsibilities. Subsequent Administration testimony indicates that DHS will receive much of the same intelligence data from other agencies and will undertake analysis. A key distinction is that DHS is not responsible for information relating to threats to U.S. interests overseas.¹⁴ In FY2004, funds were appropriated for 206 intelligence analysts in IAIP; the Administration requested 225 for FY2005.

Some observers express concern that the DCI's role in the TTIC — responsibility for the analysis of domestically collected information and for maintaining "an up-to-date database of known and suspected terrorists that will be accessible to federal and non-

¹⁰ Testimony of Bill Parrish, Acting Assistant Secretary for Information Analysis, DHS, before a Joint Hearing of the House Judiciary and Select Homeland Security Committees, July 22, 2003, Federal News Service Transcript.

¹¹ White House Fact Sheet, "Strengthening Intelligence to Better Protect America," January 28, 2003.

¹² Testimony of Bill Parrish, July 22, 2003.

¹³ U.S. Congress, House of Representatives, Select Committee on Homeland Security, "New Terror Intel Center No Substitute for Homeland Security Department Role," Press Release, May 2, 2003.

¹⁴ Testimony of Bill Parrish, July 22, 2003.

federal officials and entities,”¹⁵ — may run counter to the statutory provision that excludes the CIA from “law enforcement or internal security functions.”¹⁶ There are also questions about transferring the FBI’s Counterterrorism Division to the DCI. Some express concern about how the TTIC under the DCI will coordinate with state and local officials and with private industry as contemplated in provisions of the House-passed version of the FY2004 intelligence authorization bill (H.R. 2417).

The relationship between DHS and TTIC is also a continuing concern to Members of Congress. Some may consider modifications of the Homeland Security Act that could affect the analytical efforts of DHS.¹⁷ Section 359 of the Intelligence Authorization Act for FY2004 (P.L. 108-177) requires that the President report on the operations of IAIP and TTIC by May 1, 2004. The report, which is to be unclassified (with the option of a classified annex), asks for a delineation of the responsibilities of IAIP and TTIC and an assessment of whether areas of overlap, if any, “represent an inefficient utilization of resources.” The President is asked to “explain the basis for the establishment and operation of the Center [TTIC] as a ‘joint venture’ of participating agencies rather than as an element of the Directorate [IAIP]....” The report is also to assess the “practical impact, if any, of the operations of the Center [TTIC] on individual liberties and privacy.”

Conclusion

Legislation creating a homeland security department recognized the crucial importance of intelligence. It proposed an analytical office within DHS that would draw upon the information gathering resources of other government agencies and of the private sector. It envisioned the DHS information analysis entity working closely with other DHS offices, other federal agencies, state and local officials, and the private sector to devise strategies to protect U.S. vulnerabilities and to provide warning of specific attacks.

The Administration appears to prefer a modification to the approach originally envisioned in the legislation that created DHS. TTIC, under the direction of the DCI, will provide the integrative analytical effort that the drafters of homeland security legislation and others in Congress have felt to be essential in light of breakdowns in communication that occurred prior to September 11, 2001. Whether TTIC is consistent with the intent of Congress in passing the Homeland Security Act and whether it is ultimately the best place for the integrative effort is current a matter of discussion in Congress. Regardless of where the integrative effort is ultimately located, the task will remain fundamentally the same. Pulling together vast amounts of data from a wide variety of sources concerning terrorist groups, analyzing them, and reporting threat warnings in time to prevent attacks is and will remain a daunting challenge.

¹⁵ Ibid.

¹⁶ 50 USC 403-3(d)(1).

¹⁷ William New, “Cox Plans Substantive Revision of Homeland Security Act,” [<http://www.govexec.com>], May 2, 2003.